

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOY EMMANUEL,

Defendant.

No. 2:19-cv-309

COMPLAINT

Plaintiff, the United States of America, by and through its undersigned attorneys, brings this complaint against Defendant JOY EMMANUEL, and alleges the following:

I. NATURE OF THIS ACTION

1. Starting as early as 2017 and continuing to the present, Defendant has conducted financial transactions with large sums of illegally obtained money, knowing that his transactions are designed to conceal the nature, source, location, ownership, and control of proceeds. Defendant's conduct includes knowingly receiving money obtained via fraud and then immediately transmitting the same money to accomplices in India.

2. Defendant conducts U.S. operations for a technical-support scheme based in India. The scheme operates by fraudulently inducing consumers, including principally elderly consumers, to purchase phony or otherwise misrepresented technical-support services related to

IV. FACTS

A. Defendant's Role in an Ongoing Technical-Support Fraud Scheme

8. Defendant conducts U.S. operations for a large-scale technical-support fraud scheme that targets victims throughout the United States. Since at least as early as 2017, telemarketers based in India have used telephone calls and the infrastructure maintained by Defendant to operate the technical-support scheme. Telemarketers working for the scheme fraudulently pose as technicians to induce consumers, including principally elderly consumers, to purchase phony or otherwise misrepresented technical-support services, and to make further payments based on additional fraudulent misrepresentations. Telemarketers contact consumers by means such as placing cold calls; paying search engines to place advertisements for technical computer services; and by using pop-up advertisements disguised as security alerts on computers or other electronic devices that direct consumers to immediately call a telephone number to protect their computer or other electronic device. The telemarketers often falsely claim to work for or be affiliated with large, well-known technology companies.

9. Once a telemarketer has a consumer on the phone, the telemarketer emphasizes the need for immediate action, and claims that the consumer's computer is at risk and that the telemarketer can assist but first needs remote access to the computer or device. Once remotely connected, the telemarketer purports to confirm the existence of a serious computer virus or other threat to the consumer's computer or device, sometimes claiming that hackers have already taken over the consumer's computer or email accounts and displaying a screen purporting to show, in real time, that the device was undergoing a further hacking attack as the telemarketer and consumer spoke. Imparting a sense of urgency, the telemarketer then claims

1 that he will install expensive and high-quality network security software to resolve the threat in
2 exchange for a substantial sum of money.

3 10. After purportedly installing high-quality network security software, the
4 telemarketer instructs the consumer to pay. Consumers are generally asked to provide their
5 personal checking-account information, which is then used to generate remotely-created checks
6 made payable to one of Defendant's bank accounts. Each consumer is charged between several
7 hundred and several thousand dollars.

8 11. At times during the scheme, consumers who have already paid Defendant once
9 for technical-support receive subsequent calls, during which telemarketers working for the
10 scheme give consumers phony new reasons they must purchase additional security software to
11 avoid serious new computer viruses or other threats to their devices.

12 12. At times during the scheme, telemarketers purport to offer refunds to victims.
13 But, instead of refunding money to victims, the telemarketers actually move money within the
14 consumers' online bank accounts to convince the victims that too much money was refunded.
15 The telemarketers then induce victims to send payments, purportedly to reimburse the "over-
16 refund." Victims have lost hundreds or thousands of dollars to such bogus refund schemes.

17 13. The scheme's perpetrators use Defendant and his U.S. corporate entity to
18 facilitate their schemes by (a) maintaining the schemes' infrastructure, including (b) receiving
19 victim payments and (c) generally providing a veneer of domestic legitimacy.

20 **B. Ongoing Banking Law Violations**

21 14. Defendant conducts financial transactions to benefit an international fraud
22 scheme, knowing that the money he receives and transmits is obtained fraudulently, and
23 knowing that his transactions are designed to conceal the scheme. Defendant receives financial

1 compensation for this conduct, often by transmitting to his accomplices 60% of the amounts
2 that he receives and keeping the remaining 40% for himself.

3 15. Beginning at least as early as 2017, Defendant has knowingly accepted tens of
4 thousands of dollars from multiple fraud victims and then transmitted most of that money to
5 accomplices in the technical-support telemarketing fraud scheme.

6 16. Between June 1, 2017, and August 3, 2018 alone, Defendant deposited over
7 \$40,000 in remotely-created checks that were returned as unpayable, for reasons that included
8 victims' closing their checking accounts to prevent unauthorized transactions; insufficient
9 funds; and victims' stopping payment on grounds of fraud.

10 **C. Defendant's Knowledge of Fraud, Intent to Conceal the Nature, Source, Location,**
11 **Ownership, or Control of Proceeds, and Intent to Evade Transaction Reporting**
Requirements

12 17. On information and belief, Defendant has engaged in the financial transactions
13 alleged in Paragraphs 14 through 16 with knowledge that the monies he receives from
14 consumers are obtained by the fraud scheme or other specified unlawful activity. On
15 information and belief, Defendant has engaged in such financial transactions knowing that the
16 transmissions are designed in whole or part to conceal or disguise the nature, source, location,
17 ownership, or control of proceeds, and has transmitted such funds to India with the intent to
18 promote the carrying on of specified unlawful activity.

19 **D. Harm to the United States**

20 18. The United States is suffering continuing and substantial injury from
21 Defendant's banking law violations.

22 19. Defendant is continuing to facilitate his banking law violations. Absent
23 injunctive relief by this Court, Defendant will continue to cause continuing and substantial
injury to the United States and victims.

COUNT I

(18 U.S.C. § 1345 – Injunctive Relief)

20. The United States re-alleges and incorporates by reference Paragraphs 1 through 22 of this Complaint as though fully set forth herein.

21. By reason of the conduct described herein, Defendant has committed, is committing, and is about to commit banking law violations as defined in 18 U.S.C. § 3322(d), including money laundering and international money laundering with the intent to promote the carrying on of specified unlawful activity in violation of 18 U.S.C. § 1956(a)(1)(A)(i) and (a)(2)(A); and money laundering and international money laundering knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity, in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and (a)(2)(B)(i).

22. Because Defendant is committing or about to commit banking law violations as defined in 18 U.S.C. § 3322(d), the United States is entitled, under 18 U.S.C. § 1345, to seek a permanent injunction restraining all future banking law violations and any other action that this Court deems just to prevent a continuing and substantial injury to the United States.

23. As a result of the foregoing, Defendant's conduct should be enjoined pursuant to 18 U.S.C. § 1345.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, United States of America, requests of the Court the following relief:

1 A. That the Court issue a permanent injunction, pursuant to 18 U.S.C. § 1345,
2 ordering that Defendant is restrained from engaging, participating, or assisting in money
3 laundering or international money laundering, and any money transmitting business; and

4 B. That the Court order such other and further relief as the Court shall deem just
5 and proper.

6
7 Respectfully submitted this 1st day of March, 2019.

8 BRIAN T. MORAN
9 United States Attorney

10 s/ Kayla C. Stahman
11 KAYLA C. STAHMAN, CA #228931
12 Assistant United States Attorney
13 United States Attorney's Office
14 700 Stewart Street, Suite 5220
15 Seattle, Washington 98101-1271
16 Phone: 206-553-7970
17 Fax: 206-553-4067
18 Email: kayla.stahman@usdoj.gov

19 GUSTAV W. EYLER
20 Acting Director
21 Consumer Protection Branch

22 JILL P. FURMAN
23 Deputy Director
 Consumer Protection Branch

s/ Daniel K. Crane-Hirsch
 DANIEL K. CRANE-HIRSCH
 CLAUDE F. SCOTT
 Consumer Protection Branch
 United States Department of Justice
 P.O. Box 386
 Washington, DC 20044
 Tel.: 202-616-8242
 Fax: 202-514-8742
 Email: daniel.crane-hirsch@usdoj.gov

Counsel for United States of America

CERTIFICATE OF SERVICE

The undersigned hereby certifies that he is an employee in the Office of the United States Attorney for the Western District of Washington and is the person of such age and discretion as to be competent to serve papers;

It is further certified that on this day, I mailed by United States Postal Service said pleading to Defendant, addressed as follows:

Joy Emmanuel
13540 Wallingford Ave N
Seattle, WA 98133-7741

Dated this 1st day of March, 2019.

/s/ Thomas Everett

THOMAS EVERETT

Paralegal

United States Attorney's Office

700 Stewart Street, Suite 5220

Seattle, Washington 98101-1271

Phone: (206) 553-7970

Fax: (206) 553-0882

E-mail: thomas.everett@usdoj.gov